

CLAIMS

What is claimed is:

1. A method for controlling the delivery of broadcast encryption content for a network cluster from a content server outside the cluster, the method comprising:
 - 5 receiving in the content server from a network device a key management block for the cluster, a unique data token for the cluster, and a encrypted cluster id; and
 - 10 calculating a binding key for the cluster in dependence upon the key management block for the cluster, the unique data token for the cluster, and the encrypted cluster id.
2. The method of claim 1 wherein calculating a binding key further comprises:
 - 5 calculating a management key from the key management block for the cluster;
 - calculating a content server device key from the management key and the content server device id;
 - decrypting the encrypted cluster id with the content server device key; and
 - 10 calculating the binding key with the management key, the unique data token for the cluster, and the cluster id.
3. The method of claim 2 wherein calculating a content server device key further comprises hashing, with a one way cryptographic hash algorithm, the management key and the content server device id.

4. The method of claim 2 wherein calculating the binding key with the management key, the unique data token for the cluster, and the cluster id further comprises hashing, with a one way cryptographic hashing algorithm, the management key, the unique data token for the cluster, and the cluster id.
- 5
5. The method of claim 1 further comprising encrypting in the network device a cluster id in dependence upon a content server device id for the content server.
6. The method of claim 5 further comprising receiving in the network device a content server device id.
7. The method of claim 5 wherein encrypting a cluster id further comprises:

calculating a content server device key; and

5 encrypting the cluster id with the content server device key.
8. The method of claim 7 wherein calculating a content server device key further comprises hashing, with a one way hash algorithm, the management key and the content server device id.
9. The method of claim 1 further comprising:

encrypting the content for the cluster with a title key;

5 encrypting the title key with the binding key; and

packaging the encrypted title key with the encrypted content for the cluster.

10. A system for controlling the delivery of broadcast encryption content for a network cluster from a content server outside the cluster, the system comprising:
- 5 means for receiving in the content server from a network device a key management block for the cluster, a unique data token for the cluster, and a encrypted cluster id; and
- 10 means for calculating a binding key for the cluster in dependence upon the key management block for the cluster, the unique data token for the cluster, and the encrypted cluster id.
11. The system of claim 10 wherein means for calculating a binding key further comprises:
- 5 means for calculating a management key from the key management block for the cluster;
- means for calculating a content server device key from the management key and the content server device id;
- 10 means for decrypting the encrypted cluster id with the content server device key; and
- 15 means for calculating the binding key with the management key, the unique data token for the cluster, and the cluster id.
12. The system of claim 11 wherein means for calculating a content server device key further comprises means for hashing, with a one way cryptographic hash algorithm, the management key and the content server device id.

13. The system of claim 11 wherein means for calculating the binding key with the management key, the unique data token for the cluster, and the cluster id further comprises means for hashing, with a one way cryptographic hashing algorithm, the management key, the unique data token for the cluster, and the cluster id.
14. The system of claim 10 further comprising means for encrypting in the network device a cluster id in dependence upon a content server device id for the content server.
15. The system of claim 14 further comprising means for receiving in the network device a content server device id.
16. The system of claim 14 wherein means for encrypting a cluster id further comprises:
- means for calculating a content server device key; and
- means for encrypting the cluster id with the content server device key.
17. The system of claim 16 wherein means for calculating a content server device key further comprises means for hashing, with a one way hash algorithm, the management key and the content server device id.
18. The system of claim 10 further comprising:
- means for encrypting the content for the cluster with a title key;
- means for encrypting the title key with the binding key; and
- means for packaging the encrypted title key with the encrypted content for the

cluster.

19. A computer program product for controlling the delivery of broadcast encryption content for a network cluster from a content server outside the cluster, the computer program product comprising:
- 5 a recording medium;
- means, recorded on the recording medium, for receiving in the content server from a network device a key management block for the cluster, a unique data token for the cluster, and a encrypted cluster id; and
- 10 means, recorded on the recording medium, for calculating a binding key for the cluster in dependence upon the key management block for the cluster, the unique data token for the cluster, and the encrypted cluster id.
20. The computer program product of claim 19 wherein means, recorded on the recording medium, for calculating a binding key further comprises:
- means, recorded on the recording medium, for calculating a management key
- 5 from the key management block for the cluster;
- means, recorded on the recording medium, for calculating a content server device key from the management key and the content server device id;
- 10 means, recorded on the recording medium, for decrypting the encrypted cluster id with the content server device key; and
- means, recorded on the recording medium, for calculating the binding key with the management key, the unique data token for the cluster, and the
- 15 cluster id.

21. The computer program product of claim 20 wherein means, recorded on the recording medium, for calculating a content server device key further comprises means, recorded on the recording medium, for hashing, with a one way cryptographic hash algorithm, the management key and the content server device id.
- 5
22. The computer program product of claim 20 wherein means, recorded on the recording medium, for calculating the binding key with the management key, the unique data token for the cluster, and the cluster id further comprises means, recorded on the recording medium, for hashing, with a one way cryptographic hashing algorithm, the management key, the unique data token for the cluster, and the cluster id.
- 5
23. The computer program product of claim 19 further comprising means, recorded on the recording medium, for encrypting in the network device a cluster id in dependence upon a content server device id for the content server.
24. The computer program product of claim 23 further comprising means, recorded on the recording medium, for receiving in the network device a content server device id.
25. The computer program product of claim 23 wherein means, recorded on the recording medium, for encrypting a cluster id further comprises:
- 5
- means, recorded on the recording medium, for calculating a content server device key; and
- means, recorded on the recording medium, for encrypting the cluster id with the content server device key.

26. The computer program product of claim 25 wherein means, recorded on the recording medium, for calculating a content server device key further comprises means, recorded on the recording medium, for hashing, with a one way hash algorithm, the management key and the content server device id.
- 5
27. The computer program product of claim 19 further comprising:
- means, recorded on the recording medium, for encrypting the content for the cluster with a title key;
- 5
- means, recorded on the recording medium, for encrypting the title key with the binding key; and
- 10
- means, recorded on the recording medium, for packaging the encrypted title key with the encrypted content for the cluster.